GitHub Actions & Workflow Generation

DevOps & Infrastructure | Intermediate

Agenda

Time	Topic
0:00–0:08	Actions model
0:08–0:18	Generate CI
0:18–0:28	Debug a failed step
0:28–0:38	Reusable and custom actions
0:38–0:50	Bounded pipeline demo
0:50–1:00	Security, `gh-aw`, lab handoff

Actions model

Part	Meaning
Workflow	YAML automation in `.github/workflows/`
Event	Trigger such as `push` or `pull_request`
Job	Steps on a runner
Step	An action or command
Secret	Sensitive value outside source
Artifact	Files retained from a job

Generate from repository facts

```
Read package.json and existing tests. Create ci.yml for pull requests and main.
Use Node.js 20, npm ci, existing lint and test scripts, npm caching, contents: read,
and a test-results artifact. Do not add dependencies or deployment steps.
```

Check every assumption against the project.

Debug with useful context

Provide the failed step, error, and workflow file. Ask for the smallest fix and the follow-up check.

```
This workflow fails at "Run tests." Here is the step output and ci.yml.
Identify the cause, propose the smallest fix, and explain what to verify.
```

Security review

- Set explicit least-privilege `permissions`.
- Keep values in secrets or use OIDC.
- Review triggers, especially `pull_request_target`.
- Pin approved third-party actions to immutable SHAs in production.
- Check commands, runners, artifacts, concurrency, and deployment gates.

```
permissions:
  contents: read
```

Agentic Workflows

```
gh extension install github/gh-aw
gh aw init daily-repo-status
gh aw compile daily-repo-status
gh aw logs daily-repo-status
```

Review Markdown source and compiled `.lock.yml`. Keep permissions read-only unless a reviewed `safe-outputs` write is required.

Lab

Build CI, design CD, fix supplied broken workflows, and create a JavaScript action. `gh-aw` is optional and requires approval.